ABSTRACT OF THE DISCLOSURE

An improved system and method for detecting spam e-mail over a distributed network is disclosed. The distributed network includes multiple servers that receive and process e-mail messages for a multiple remotely located clients. The system includes multiple packet sniffers that are each located on a unique one of servers. The packet sniffers extract originating IP addresses associated with e-mail messages that are communicated to the clients over the network. The system further includes a central monitor that communicates with the packet sniffers and that monitors data regarding originating IP addresses. The monitor determines whether an originating IP address has exceeded a threshold value and may take corrective measures in response, such as generating an alert to a spam analyst or blocking messages originating from that IP address. By leveraging data from several different clients, the system can detect and stop spam messages for an IP address even if a spammer has not targeted a specific customer.